VOL. 12, NO. 4, FEBRUARY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DATA MINING BASED APPROACH FOR ROUTING ANOMALY DETECTION IN MANET

S. B. Ninu[1] and S. Behin Sam[2]
[1]Department of Computer Science, Bharathiar University, Thiruthangal Nadar College, Selvayal, Chennai, India
[2]Department of Computer Science, R. V. Government Arts College, Chengalpattu, India
E-Mail: behinsam@gmail.com

ABSTRACT

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. Anomalous route request and route reply will cause severe damage in the communication process. In order to identify these types of anomalies, MANETs require the use of data mining to extract information and patterns derived by the knowledge in routing process. In this paper we present a data mining based anomaly detection system which will identify two types of routing anomalies or attacks. The first one is false route request attack and the second one is false route reply attack. We show that the proposed method provides significant prediction accuracy.

Keyword: MANET, anomaly detection, data mining, artificial neural network.

INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are a collection of heterogeneous, infrastructure less, self organizing and battery powered mobile nodes with different resources availability and computational capabilities. The dynamic and distributed nature of MANETs makes them suitable for deployment in extreme and volatile environmental conditions. They have found applications in diverse domains such as military operations, environmental monitoring, rescue operations etc. Each node in a MANET is equipped with a wireless transmitter and receiver, which enables it to communicate with other nodes within its wireless transmission range.

However, due to limited wireless communication range and node mobility, nodes in MANET must cooperate with each other to provide networking services among themselves. Therefore, each node in a MANET acts both as a host and a router. The dynamic and distributed nature of MANETs make them vulnerable to various types of attacks like black hole attack, traffic distortion, IP spoofing, DoS attack etc. Malicious nodes can launch attacks against other normal nodes and deteriorate the overall performance of the entire network (A. Mishra *et al*., 2004, Y. Zhang *et al*., 2003, M. La Polla *et al*., 2013). Unlike in wired networks, there are no fixed checkpoints like router and switches in MANETs, where the Intrusion Detection System (IDS) can be deployed (F. Anjum and P. Mouchtaris, 2006, P. Brutch and C. Ko, 2003). Therefore, nodes in MANETs must cooperate in many aspects including intrusion detection for their well being (Y.-C. Hu *et al*., 2005, S. Bu *et al*., 2011, Z. Fadlullah *et al*., 2013). IDSs have been deployed with great degree of success across diverse domains like wireless Ad-hoc networks (P. Brutch and C. Ko, 2003, Y. Zhang and W. Lee, 2000), MANETs (T. Anantvalee and J. Wu, 2007, A. Mitrokotsa and C. Dimitrakakis, 2013, C. Xenakis *et al*., 2011), wireless sensor networks I Butun *et al*., 2014, cyber-physical system R. Mitchell and I. Chen, 2013, cloud computing A. Patel *et al*., 2013, large scale complex critical infrastructures C.E. Perkins *et al*., 2002 etc.

In recent years, data mining techniques have been successfully used in the context of network intrusion detection. They have been extensively used in discriminating normal behavior from abnormal behavior in a variety of contexts. Data mining has become a very useful technique to reduce information overload and improve decision making by extracting and refining useful knowledge through a process of searching for relationships and patterns from the extensive data collected by organization. The extracted information is used to predict, classify, model, and summarize the data being mined. Data mining technologies, such as rule induction, neural networks, genetic algorithms, fuzzy logic, and rough sets are used for classification and pattern recognition.

In this paper, we propose an IDS for MANETs based on a dataminig algorithm called as Adaptive Neuro-Fuzzy Inference System (ANFIS) P.Arun Rajkumar and S. Selvakumar, 2013, that will detect false route request attack and false route reply attack.

METHODOLOGY

The proposed IDS, is used to detect intrusion packets while the communication is taking place. This IDS module is used to identify false route request and false route reply attack. The architecture for intrusion detection module is depicted in the Figure-1.

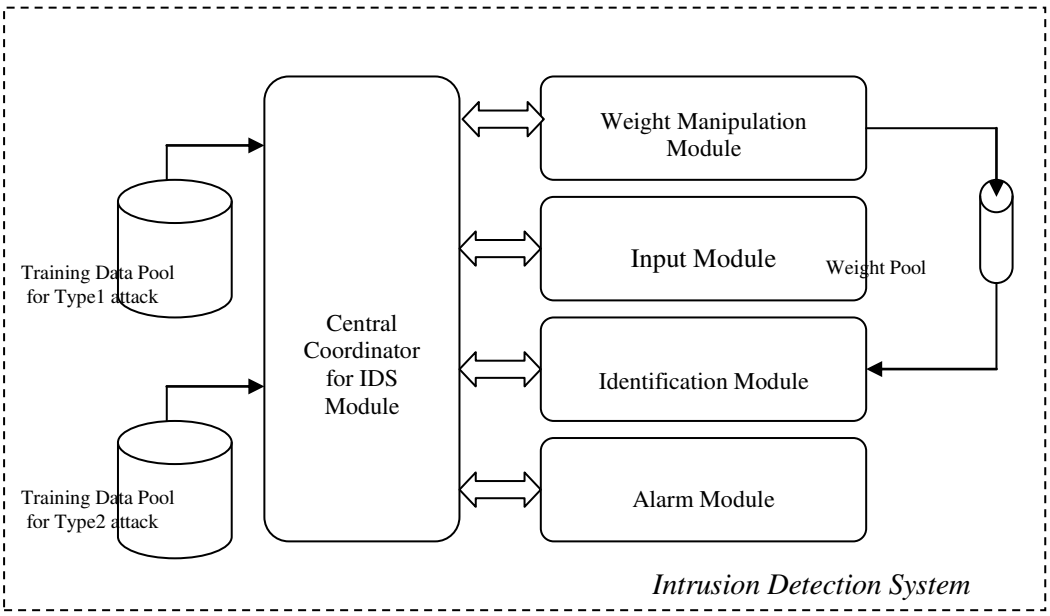

Figure-1. System architecture for IDS.

The IDS system here uses the Adaptive Neuro-Fuzzy Inference System to analyze the incoming data packets for detecting the two types of attacks. Type 1 attack is called as false route request attack and Type 2 attack is called as false route reply attack. The algorithm used for training and testing is given below:

RESULTS AND DISCUSSIONS

Packets are generated in NS 2.35 for training, validation and testing. The data set contains packets of three types. The first type of packets is the normal packet. The second one is false route request packet. The final one is false route reply packet. For simulation, 2900 packets are generated for training set, 900 packets are generated for validation set and 700 packets are generated for test set. The details of these data sets are given in Table-1.

Table-1. Total number of packets for training, validation and testing.

Packet type	Training set	Validation set	Test set
Normal	1200	300	250
Infected Type 1	800	300	250
Infected Type 2	900	300	200

Because of the stochastic nature of the neural networks, it is usually common to report the results of multiple training-testing procedures. Table-2 illustrates the results of three training-validation-testing sessions.

Table-2. Average classification rates for three different training and test sessions.

Training/Testing session	Correct classification on training set	Correct classification on test set
1	98.20	89.20
2	98.10	90.90
3	96.90	90.30
Average	97.46	90.13

The results shown in Table-2 clearly show that on the average, the ANN based intrusion detection system is able to classify attacks 90% correctly.

IDS ALGORITHM

Input:

For each dataset DS_j, where j=1,2 and3 representing Normal, Type1 and Type 2 attack

- Training data TD_j of size N with correct lables
- Neural Network Classifier
- Number of iterations or classifiers (T)
- Number of classes (L)=(Ω1, Ω2, Ω3)

Initialize:

- μ = 0.5 // False Alarm Threshold
- L=3 // Number of classes (Normal, Type1 and Type 2 attack)
- $d_t(i) = \frac{1}{n}$ // Summing up all instance weights results in unity

Training:

Do for j-1….L

1. Choose samples from calss j and from data source DS_j
2. Split DS_j into k subsets $S_1, S_2, \ldots\ldots S_k$

Do for each m = 1….k

Do for t = 1…….T

a) Train $S_m$by ANFIS and obtain hypothesis h_t

b) Compute error of h_t: $\in_t = \frac{\sum_{i=1}^{n}[h_t(x_i) \neq y_i]}{n}$

c) If $\in_t = \mu$, then drop hypothesis and go to step 2.a
Else add the classifier h_t to the collection C_m

d) Compute normalized error $\beta_t = \frac{\in_t}{1-\in_t}$, $0 < \beta_t < 1$

e) Assign weights to the classifier $w_t = \log\frac{1}{\beta_t}$

f) $\beta_{tt} = \beta_t * \mu$

g) Update distribution of instances

$$d_{t+1}(i) = d_t(i)\begin{cases}\beta_{tt}, \text{if } h_t(x_i) = y_i \\ 1, \text{if } h_t(x_i) \neq y_{i\ and\ if\ y_i \in \Omega 1} \\ \mu, \text{if } h_t(x_i) \neq y_i\end{cases}$$

End

Obtain Composite Hypothesis $H_j^m = \arg mean \sum_{t=1}^{n} \log\frac{1}{\beta_t^m}$

End

End

Testing:

Given an unlabeled instance 'X'

A) Evaluate the collection C_m of each data subset for particular class on X
B) Obtain composite hypothesis for each subset by weighted mean
C) Find the class based on the threshold value
D) Obtain the total vote received by each class
E) Choose the class that has the highest total vote as the final classification decision

CONCLUSIONS

In this paper we have proposed and IDS for MANE which can detect routing anomaly. This IDS use a data mining approach based on Adaptive Neuro-Fuzzy Inference System for classification. The performance of the IDS was evaluated based on the testing dataset which contains attack types not included in the training set. From the simulation experiments, it was evident that the trained IDS were able to detect new attacks. Hence, the Learning module learns the new data without forgetting the previously acquired knowledge, discarding the existing classifier, and retraining a new one. The IDS algorithm can deal with both discrete and continuous attributes in the database, which is practically useful for real time network datasets. Hence our IDS are suitable for real time

deduction of false route request and false route reply attacks.

REFERENCES

[1] A. Mishra, K. Nadkarni, A. Patcha. 2004. Intrusion detection in wireless Ad-hoc networks, IEEE Wirel. Commun. 11(1): 48-60.

[2] Y. Zhang, W. Lee, Y.-A. Huang. 2003. Intrusion detection techniques for mobile wireless networks, Wirel. Netw. 9(5): 545-556.

[3] M. La Polla, F. Martinelli, D. Sgandurra. 2013. A survey on security for mobile devices. IEEE Commun. Surv. Tutor. 15(1): 446-471.

[4] F. Anjum, P. Mouchtaris. 2006. Intrusion Detection Systems, John Wiley and Sons, Inc.

[5] P. Brutch, C. Ko. 2003. Challenges in intrusion detection for wireless ad-hoc networks, in: Proceedings of Symposium on Applications and the Internet Workshops. pp. 368-373.

[6] Y.-C. Hu, A. Perrig, D. Johnson. 2005. Ariadne: a secure on-demand routing protocol for ad-hoc networks, Wirel. Netw. 11(1-2): 21-38.

[7] S. Bu, F. Yu, X. Liu, P. Mason, H. Tang. 2011. Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE Trans. Veh. Technol. 60(3): 1025-1036.

[8] Z. Fadlullah, H. Nishiyama, N. Kato, M. Fouda. 2013. Intrusion detection system (IDS) for combating attacks against cognitive radio networks, IEEE Netw. 27(3): 51-56.

[9] Y. Zhang, W. Lee. 2000. Intrusion detection in wireless ad-hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM. pp. 275-283.

[10] T. Anantvalee, J. Wu. 2007. A survey on intrusion detection in Mobile Ad Hoc Networks, in: Wireless Network Security, Signals and Communication Technology, Springer. pp. 159-180.

[11] A. Mitrokotsa, C. Dimitrakakis. 2013. Intrusion detection in MANET using classification algorithms: the effects of cost and model selection, Ad Hoc Netw. 11(1): 226-237.

[12] C. Xenakis, C. Panos, I. Stavrakakis. 2011. A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, Comput. Secur. 30(1): 63-80.

[13] I. Butun, S. Morgera, R. Sankar. 2014. A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. 16(1): 266-282.

[14] R. Mitchell, I. Chen. 2013. Effect of intrusion detection and response on reliability of cyber physical systems. IEEE Trans. Reliab. 62(1): 199-210.

[15] A. Patel, M. Taghavi, K. Bakhtiyari, J.C. Jnior. 2013. An intrusion detection and prevention system in cloud computing: a systematic review, J. Netw. Comput. Appl. 36(1): 25-41.

[16] C.E. Perkins, E.M. Royer,S. R.Das. 2002. Adhoc on demand distance vector (AODV) routing. IETF INTERNET DRAFT, MANET working group.

[17] P. Arun Rajkumar, S. Selvakumar. 2013. Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems, Computer Communications. 36: 303-319.